PCT/JP2004/004138

日本国特許庁
JAPAN PATENT OFFICE

25. 3. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２６日

出願番号
Application Number: 特願２００３－０８５０４３

[ST. 10/C]: ［ＪＰ２００３－０８５０４３］

出願人
Applicant(s): 松下電器産業株式会社

２００４年　４月２８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０３６６５４

【書類名】　特許願
【整理番号】　2113140223
【提出日】　平成15年 3月26日
【あて先】　特許庁長官殿
【国際特許分類】　H04N 7/167
H04K 1/00
G06F 12/14 320
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　鈴木　秀和
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100097445
【弁理士】
【氏名又は名称】　岩橋　文雄
【選任した代理人】
【識別番号】　100103355
【弁理士】
【氏名又は名称】　坂口　智康
【選任した代理人】
【識別番号】　100109667
【弁理士】
【氏名又は名称】　内藤　浩樹
【手数料の表示】
【予納台帳番号】　011305
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】明細書

【発明の名称】　リボケーション情報の送信方法、受信方法及びその装置

【特許請求の範囲】

【請求項１】　コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ機器と前記コンテンツ受信機器とを接続する接続手段から構成されるシステムにおいて、前記コンテンツ送出機器とコンテンツ受信機器が相互認証を行なうステップと、相互認証が失敗の場合、前記コンテンツ送出機器または前記コンテンツ受信機器から、相互認証に失敗した鍵情報を含むリボケーション情報をアップロードするステップと、複数のコンテンツ送出機器またはコンテンツ受信機器からアップロードされた個々のリボケーション情報を統合して統合リボケーション情報を作成するステップと、前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、前記統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とするリボケーション情報の送信方法。

【請求項２】　１個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合して統合リボケーション情報を作成するステップと、前記統合リボケーション情報を前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、前記統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とするリボケーション情報の送信方法。

【請求項３】　統合リボケーション情報をＭＰＥＧトランスポートストリームのセクションのデータ構造を用いて伝送することを特徴とする請求項１または請求項２に記載のリボケーション情報の送信方法。

【請求項４】　統合リボケーション情報をＭＰＥＧトランスポートストリームのＰＥＳパケットのデータ構造を用いて伝送することを特徴とする請求項１または請求項２に記載のリボケーション情報の送信方法。

【請求項５】　統合リボケーション情報をＭＰＥＧトランスポートストリームのトランスポートパケットのペイロードを用いて伝送することを特徴とする請求項１または請求項２に記載のリボケーション情報の送信方法。

【請求項６】　統合リボケーション情報をＩＰパケットを用いて伝送することを特徴とする請求項１または請求項２に記載のリボケーション情報の送信方法。

【請求項７】　コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とするリボケーション情報の受信方法。

【請求項８】　コンテンツを送出する複数のコンテンツ送出機器と、前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受信する複数のコンテンツ受信機器と、前記コンテンツ送出機器と前記コンテンツ受信機器とを接続する接続手段と、前記複数のコンテンツ送出機器または前記複数の受信機器からリボケーション情報を吸い上げるネットワークと前記ネットワークに接続され、リボケーション情報を統合する統合手段と、前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、前記多重化手段において多重されたストリームを送信する送信手段とを備えることを特徴とするリボケーション情報の送信装置。

【請求項９】　１個または複数のコンテンツ送出機器またはコンテンツ受信機器のリボケーション情報を統合する統合手段と、前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、

前記多重化手段において多重されたストリームを送信する送信手段とを備えることを特徴とするリボケーション情報の送信装置。

【請求項１０】　統合リボケーション情報をＭＰＥＧトランスポートストリームのセクションのデータ構造を用いて伝送することを特徴とする請求項８または請求項９に記載のリボケーション情報の送信装置。

【請求項１１】　統合リボケーション情報をＭＰＥＧトランスポートストリームのＰＥＳパケットのデータ構造を用いて伝送することを特徴とする請求項８または請求項９に記載のリボケーション情報の送信装置

【請求項１２】　統合リボケーション情報をＭＰＥＧトランスポートストリームのトランスポートパケットのペイロードを用いて伝送することを特徴とする請

求項８または請求項９に記載のリボケーション情報の送信装置。

【請求項１３】　統合リボケーション情報をＩＰパケット用いて伝送することを特徴とする請求項８または請求項９に記載のリボケーション情報の送信装置。

【請求項１４】　コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とするリボケーション情報の受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、デジタル映像やデジタル音声を不当な電子機器で表示したり、再生したりすることを防止するためのリボケーション情報の配信方法及び装置に関するものである。

【０００２】

【従来の技術】

近年、デジタル技術の発展に伴って、デジタル放送やインターネットによるデジタルコンテンツの配信や、ＤＶＤやハードディスクやメモリカードによるデジタルコンテンツの配布や蓄積が盛んに行なわれている。これらのメディアではデジタルデータを用いるので、その品質を劣化させることなくコピーを行なうことが可能であるが、著作権保護の観点からその不正なコピーを防ぐためのセキュリティの実現が重要である。セキュリティの実現のためには、著作権保護上、不正な機器が発覚した場合、不正機器のいわゆるブラックリストであるリボケーション情報を発行し、不正な機器に接続されうる機器がそのリボケーション情報を持ち、デジタルコンテンツへの不正なアクセスを防ぐ必要がある。

【０００３】

リボケーション情報の更新に関する従来例のシステムの構成を図２５に示す（特許文献１参照）。

【０００４】

１はコンテンツ販売システムで、放送やインターネットの通信網を介して音楽

コンテンツを電子配信する自動販売機である。２はＥｌｅｃｔｒｉｃ　ＭＵＳＩＣ　Ｄｉｓｔｒｉｂｕｔｅｒ（ＥＭＤ）で音楽サーバーや音楽放送局である。３はリボケーション情報発行機関である。４はセキュアコンテンツサーバーである。５はリボケーション情報格納部で、リボケーション情報発行機関が発行したリボケーション情報を受け取る。６は音楽データ格納部で、音楽データを格納する。７はライセンス格納部で、暗号化コンテンツを復号するためのキーを格納する。８はＥＭＤ　Ｉ／Ｆ部で暗号化コンテンツを受け取るためのインタフェースである。９はＰＤ　Ｉ／Ｆ部でＰＤ１２と接続するためのインタフェースである。１０はメディアイＩ／Ｆ部でＰＭ１３を装着するためのＰＣＭＣＩＡのカードスロットである。１１は記憶メディアで、Ｐｏｒｔａｂｌｅ　Ｍｅｄｉａ（ＰＭ）である。１２は記憶再生装置ＰＤである。１３はユーザＩ／Ｆ部でユーザが操作を行うインタフェースである。

【０００５】

【特許文献１】

特開２００１－１６６９９６号公報

【０００６】

【発明が解決しようとする課題】

しかし、この従来例ではリボケーション情報の更新方法については述べられているが、リボケーション情報を配布する具体的方法がないため、デジタル放送やインターネットでのコンテンツ配信が高まりを見せる状況で、リボケーション情報の配信するためのが必要である。

【０００７】

【課題を解決するための手段】

本発明は上記の問題点を解決するためになされたもので、本発明（請求項１）にかかるリボケーション情報の送信方法は、コンテンツを送出するコンテンツ送出機器と、コンテンツ受信するコンテンツ受信機器と、前記コンテンツ機器と前記コンテンツ受信機器とを接続する接続手段から構成されるシステムにおいて、前記コンテンツ送出機器とコンテンツ受信機器が相互認証を行なうステップと、相互認証が失敗の場合、前記コンテンツ送出機器または前記コンテンツ受信機器

から、相互認証に失敗した鍵情報を含むリボケーション情報をアップロードするステップと、複数のコンテンツ送出機器またはコンテンツ受信機器からアップロードされた個々のリボケーション情報を統合して統合リボケーション情報を作成するステップと、前記統合リボケーション情報をパケット化し、ストリームに多重するステップと、前記統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とする。

【０００８】

また本発明（請求項７）にかかるリボケーション情報の受信方法は、コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とする。

【０００９】

また、本発明（請求項８）にかかるリボケーション情報の送信装置は、コンテンツを送出する複数のコンテンツ送出機器と、前記複数のコンテンツ送出機器にそれぞれ接続され、コンテンツを受信する複数のコンテンツ受信機器と、前記コンテンツ送出機器と前記コンテンツ受信機器とを接続する接続手段と、前記複数のコンテンツ送出機器または前記複数の受信機器からリボケーション情報を吸い上げるネットワークと前記ネットワークに接続され、リボケーション情報を統合する統合手段と、前記統合手段において統合された統合リボケーション情報をパケット化してストリームに多重する多重化手段と、前記多重化手段において多重されたストリームを送信する送信手段とを備えることを特徴とする。

【００１０】

また、本発明（請求項１４）にかかるリボケーション情報の受信装置は、コンテンツ送出機器またはコンテンツ受信機器が統合リボケーションリストを受信し、前記コンテンツ送出機器または前記コンテンツ受信機器が前記統合リボケーションリストを記憶することを特徴とする。

【００１１】

【発明の実施の形態】

（実施の形態１）

以下、図面を参照しながら本発明のリボケーション情報の送信方法、受信方法の実施の形態１について説明する。図１は本発明の実施の形態１におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す図である。１０１～１０９は各家庭にある民生機器である。１０１は第１のディスプレイで、ＣＲＴや液晶ディスプレイ、プラズマディスプレイ等で映像を表示するもので、スピーカも備え音声を出力する場合もある。

【００１２】

図２に第１のディスプレイ１０１の内部構成を示す。１００１は表示部で映像を表示するものである。１００２は機器インタフェースで後述するＳＴＢと接続するものである。１００３はディスプレイのコントロール部で、ディスプレイ全体の制御を行うものである。１００４はメモリ部で、後述するディスプレイのメーカＩＤや機器ＩＤや鍵情報を格納するものである。

【００１３】

１０２は第１のＳＴＢ（セットトップボックス）で、配信または放送されるデジタルの映像や音声その他のデータを受信し、復号、再生を行うものである。ここではデジタル放送を受信するＳＴＢとする。

【００１４】

図３にＳＴＢの内部構成を示す。１１０１はアンテナでデジタル放送の電波を受信するものである。１１０２はチューナー部で、放送波の復調を行うものである。１１０３はフロントエンド部で、復調された信号に対して、誤り訂正等を行いＴＳ（トランスポートストリーム）を再生するものである。１１０４はＴＳデコーダ部で、複数の番組が多重されたＴＳからユーザが選択した番組のパケット（映像、音声、データ等）を抽出するものである。１１０５はＡＶデコーダ部で、ＴＳデコーダ部１１０４で抽出した映像パケット及び音声パケットの伸張を行い、デジタルの映像信号及び音声信号を出力するものである。１１０６はコントロール部で、ＳＴＢの全体の制御を行うものである。１１０７はメモリ部で後述するリボケーションリストやＳＴＢの鍵情報など格納するものである。１１０８はディスプレイインタフェースで映像、音声をディスプレーに向けて出力したり、鍵情報を交換したりするためのものである。１１０９はモデム部で、後述する

ネットワーク１１３と通信するためのものである。

【００１５】

１０３は第１のディスプレイと第１のＳＴＢを接続するデジタルインタフェースであり、ここでは例としてＨＤＭＩ（Ｈｉｇｈ－Ｄｅｆｉｎｉｔｉｏｎ Ｍｕｌｔｉｍｅｄｉａ Ｉｎｔｅｒｆａｃｅ）とする。１０４は第２のディスプレイで、第１のディスプレイ１０１と同様なものである。１０５は第２のＳＴＢで、第１のＳＴＢ１０２と同様なものである。１０６は第２のディスプレイと第２のＳＴＢを接続する第２のデジタルインタフェースで、第１のデジタルインタフェース１０３と同一である。

【００１６】

１０７は第Ｎのディスプレイ（Ｎは自然数）で、第１のディスプレイ１０１と同様なものである。１０８は第ＮのＳＴＢで、第１のＳＴＢ１０２と同様なものである。１０９は第Ｎのデジタルインタフェースで、第１のデジタルインタフェース１０３と同様なものである。

【００１７】

１１０は第１のＳＴＢ１０２と後述するネットワークとを接続する第１の上り回線で、ＳＴＢに蓄積したリボケーションリストをネットワークに送信するための媒体である。リボケーションリストについては後で説明する。上り回線には銅線や光ケーブル等がある。

【００１８】

１１１は第２の上り回線で、第１の上り回線１１０と同様なものである。１１２は第Ｎの上り回線で、第１の上り回線１１０と同様なものである。１０１～１１２は各家庭に存在するものまたは、各家庭個別に対応するものであり、Ｎの値は限定されるものではない。

【００１９】

１１３はネットワークで、各家庭のＳＴＢからリボケーションリストのリボケーションリスト統合部に吸い上げるための媒体であり、例えば電話網やインターネットなどがある。１１４はリボケーションリスト統合部で各ＳＴＢから吸い上げられたリボケーションリストを統合して、リボケーションリストの一覧である

統合リボケーションリストの作成及び管理を行うものである。１１５は送出センターで、統合されたリボケーションリストをパケット化して放送用のトランスポートストリームに多重するものである。１１６は送信部で、各ＳＴＢに送信するもので、例えば送信アンテナである。

【００２０】

以上のように構成された実施の形態１についてその動作を説明する。ＨＭＤＩではＨＤＣＰ（Ｈｉｇｉ－Ｂａｎｄｗｉｄｔｈ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）という暗号化システムが用いられる。ＨＤＣＰは、ＳＴＢやＤＶＤといった映像や音声を送出する送出機器と、ディスプレイなど映像を表示する受信機器との間に流れるデジタルコンテンツの暗号化方法を規定する。詳細はＨＤＣＰの規格書である、Ｈｉｇｉ－Ｂａｎｄｗｉｄｔｈ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ、に詳述されており説明を省略する。

【００２１】

第１～第Ｎのディスプレイは、それぞれのメモリ部１１０４に、メーカーＩＤ、機器ＩＤ及び５６ビット×４０行のディスプレイ用のデバイスキーの行列を有している。この様子を図４に示す。また、このデバイスキーの行列に対応して、個々のデバイスキーの行を指定するためのキーセレクションベクトル（以下ＫＳＶと略す）が割り当てられ、メモリ部１１０７に格納されている。以降、ディスプレイ用のＫＳＶをＢｋｓｖと記す。

【００２２】

また第１～第ＮのＳＴＢもそれぞれのメモリ部１００４にＳＴＢ用のデバイスキーとＫＳＶを有している。以降、ＳＴＢ用のＫＳＶをＡｋｓｖと記す。

【００２３】

デバイスキーもキーセレクションベクトルも、ＨＤＣＰの管理組織であるＬＬＣが管理し、各ディスプレイやＳＴＢやＤＶＤといった各機器に付与する。

【００２４】

次に各ＳＴＢでのリボケーションリストの作成の方法について説明する。例として、第１のＳＴＢ１０２と第１のディスプレイ１０１について説明する。図５

にＳＴＢとディスプレイの初期認証の処理を示す。この処理の詳細は先述した文献Ｈｉｇｉ－Ｂａｎｄｗｉｄｔｈ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍに述べられており、説明を省略する。第１のＳＴＢがメモリ部１１０７に有しているリボケーションリストの例を図６に示す。このリストには、著作権保護上、不正機器として排除すべきディスプレイのメーカーＩＤ、機器ＩＤ、Ｂｋｓｖが格納されており、図６の例では２個のディスプレイが排除されるべき機器として登録されている。メーカーＩＤはメーカを識別するものである。機器ＩＤは機器を識別するもので例えば機器のシリアルナンバーである。

【００２５】

以下、初期認証について説明する。まず、第１のＳＴＢ１０２と第１のディスプレイ１０１が第１のデジタルインタフェース１０３で接続されるか、または第１のＳＴＢ１０２と第１のディスプレイ１０１に電源が投入される。

【００２６】

次に第１のＳＴＢ１０２は第１のディスプレイ１０１からメーカーＩＤ、機器ＩＤ、Ｂｋｓｖを第1のデジタルインタフェース１０３を介して読み出す。このとき、第１のデジタルインタフェースの制御線であるＩ２Ｃラインを用いればよい。

【００２７】

ここで、読み出したメーカーＩＤ、機器ＩＤ、Ｂｋｓｖが第１のＳＴＢが持っているリボケーションリストに同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

【００２８】

次に、第１のＳＴＢ１０２から第１のディスプレイ１０１に対して、６４ビットの乱数Ａｎと、Ａｋｓｖを第１のデジタルインタフェース１０３経由で書き込む。

【００２９】

ここでもＩ２Ｃラインを用いればよい。

【００３０】

次に、第１のＳＴＢ１０２は第１のディスプレイ１０１からＢｋｓｖを読み出し、第１のＳＴＢで、下記（数１）の演算を行なう。

【００３１】

【数１】

$$Km = \Sigma Akeys\ over\ Bksv$$

【００３２】

（数１）の演算を説明する。ＡｋｅｙｓはＳＴＢのメモリ部１１０７に格納されている５６ビット×４０行のＳＴＢのデバイスキーの行列である。例えばＢｋｓｖを１６進数表現で０×２Ｂ８とすれば、ゼロ始まりでのビット位置３，４，５，７，９のみ１であとは０である。

【００３３】

そして、上の式はＢｋｓｖの１が存在するビット位置３，４，５，７，９を行のインデクスとして、５個の５６ビットのキーを加算したものである。

【００３４】

第１のディスプレイ１０１でも、同様に下記（数２）の演算を行なう。

【００３５】

【数２】

$$Km' = \Sigma Bkeys\ over\ Aksv$$

【００３６】

Ｂｋｅｙｓはディスプレイのメモリ部１００４に格納されている５６ビット×４０行のディスプレイのデバイスキーの行列である。

【００３７】

次にＳＴＢではＫｍをもとにして、下記（数３）の演算を行ない、Ｋｓ、Ｍ０、Ｒ０を得る。

【００３８】

【数３】

$$(Ks, M0, R0) = hdcpBlkCipher(Km, REPEATER \mid\mid An)$$

【００３９】

（数３）でＲＥＰＥＡＴＥＲは該当する機器がリピート機能、つまり再送信機

能を果たす場合に１で、それ以外の場合は０である。ここではディスプレイがリピート機能を有さないとし、０とする。また（数３）で||はビットの連結を示す。（数３）で用いられるｈｄｃｐＢｌｋＣｉｐｈｅｒという演算子については、文献Ｈｉｇｉ－Ｂａｎｄｗｉｄｔｈ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍの４．５節に詳述されているので説明を省略する。

【００４０】

一方、ディスプレイでも同様に下記（数４）の演算を行なう。

【００４１】

【数４】

$$(Ks', M0', R0') = hdcpBlkCipher(Km', REPEATER \,||\, An)$$

【００４２】

次に初期認証の判定処理を行なうが、この様子を図７に示す。ＳＴＢはディスプレイからＲ０´を読み出し、Ｒ０＝Ｒ０´であるかどうかを判定する。もしＲ０とＲ０´が一致すれば、初期認証は成功である。一方、Ｒ０とＲ０´が一致しなければ、初期認証は失敗とし、ＳＴＢはメモリ部１１０７のリボケーションリストにディスプレイのＢｋｓｖを違反しているものとして登録する。このとき、メーカーＩＤと機器ＩＤも併せて格納する。その場合のメモリ部１１０７の様子を図８に示す。図８において、ｍａｋｅｒ＿３、ｋｉｋｉ＿３、Ｂｋｓｖ＿３が新た不正機器として登録されたものである。

【００４３】

以上の初期認証処理の詳細は文献Ｈｉｇｉ－Ｂａｎｄｗｉｄｔｈ　Ｄｉｇｉｔａｌ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍに詳述されているので説明を省略する。　第２～第ＮのＳＴＢ、第２～第Ｎのディスプレイでも、第１のＳＴＢ、第１のディスプレイと同様な初期認証処理を行ない、違反しているBksvがあれば、それらに接続されたＳＴＢのメモリ部のリボケーションリストに登録する。

【００４４】

次に各ＳＴＢに登録されているリボケーションリストを統合して、各ＳＴＢに

送信する方法について説明する。図９にリボケーションリストのアップロード～送出までのフローを示す。

【００４５】

ステップ１０１において、

ＳＴＢのコントロール部１１０６が、メモリ部１１０７に格納されたリボケーションリストからメーカーＩＤ、機器ＩＤ、Bksvを読み出し、モデム部１１０９に転送する。

【００４６】

ステップ１０２において、

ＳＴＢのモデム部１１０９から上り回線１１０、ネットワーク１１３経由でBksvをリボケーションリスト統合部１１４にアップロードする。

【００４７】

ステップ１０３において、

リボケーションリスト統合部１１４において、所定期間に各ＳＴＢからアップロードされたBksvのリストを作成し、これを統合リボケーションリストとする。

【００４８】

ステップ１０４において、

リボケーションリスト統合部１１４から送出センター１１５に統合リボケーションリストを伝送する。

【００４９】

ステップ１０５において、

送出センター１１５で統合リボケーションリストをパケット化して、トランスポートストリームに多重する。

【００５０】

ステップ１０６において、

送信部１１６より、統合リボケーションリストが多重されたトランスポートストリームを各ＳＴＢに送信する。

【００５１】

ここでステップ１０５におけるリボケーションリストのパケット化及び多重化

について詳細に説明する。図１０にトランスポートパケットの模式図を示し、図１１にトランスポートパケットのデータ構造を示す。トランスポートパケットのデータ構造は、ＭＰＥＧシステム規格書であるＩＳＯ／ＩＥＣ１３８１８－１に述べられているので省略する。

【００５２】

統合リボケーションリストはトランスポートパケットのペイロード部分すなわち、図１０のｄａｔａ＿ｂｙｔｅの部分に格納し、ある所定のＰＩＤを割り当てる。このＰＩＤを仮にＲｅｖｏｃａｔｉｏｎ＿ｐｉｄとする。実施の形態１では統合リボケーションリストはＭＰＥＧシステム規格のセクション構造に格納する。図１１に統合リボケーションリストをセクション構造に格納した場合のデータ構造の例を示す。統合リボケーションリストのテーブルを仮にＲｅｖｏｃａｔｉｏｎ＿ｌｉｓｔ＿ｔａｂｌｅと称するが、もちろん、他の名前であっても構わない。このデータ構造において、ｍａｋｅｒ＿ｉｄ（１６ビット）、ｋｉｋｉ＿ｉｄ（３２ビット）、ｄｅｖｉｃｅ＿ＫＳＶ（４０ビット）がＳＴＢから吸い上げた、メーカーＩＤ、機器ＩＤ、違反した個々のＢｋｓｖである。ただし、メーカーＩＤ、機器ＩＤは何ビットであっても構わない。

【００５３】

次に、各ＳＴＢにおける統合リボケーションリストの受信の方法について説明する。図１３にＳＴＢでの統合リボケーションリストの受信フローを示す。

【００５４】

ステップ２０１において、

ＳＴＢがＲｅｖｏｃａｔｉｏｎ＿ｌｉｓｔ＿ｔａｂｌｅを含むＴＳ（トランスポートストリーム）を受信する。

【００５５】

ステップ２０２において、

ＳＴＢのＴＳデコーダ部１１０４でＴＳからＲｅｖｏｃａｔｉｏｎ＿ｌｉｓｔ＿ｔａｂｌｅを含むパケットを抽出するように、コントロール部１１０６は、ＴＳデコーダ部１１０４にＰＩＤフィルタにＲｅｖｏｃａｔｉｏｎ＿ｐｉｄを設定する。ＰＩＤフィルタとは、指定したＰＩＤを持ったパケットを抽出するたもの

でＴＳデコーダには必須の機能ある。

【００５６】

ステップ２０３において、

ＴＳデコーダ部でＲｅｖｏｃａｔｉｏｎ＿ｌｉｓｔ＿ｔａｂｌｅを含むパケットを抽出し、コントロール部１１０６が統合リボケーションリストを取得する。

【００５７】

ステップ２０４において、

コントロール部１１０６は取得した統合リボケーションリストを、メモリ部１１０７に格納する。

【００５８】

メモリ部１１０７に格納された統合リボケーションリストを図１４に示す。これにより、すべてのＳＴＢで統合リボケーションリストを共有することが可能になる。

【００５９】

そして、新たなディスプレイがＳＴＢに接続された場合に、ディスプレイから読み出したメーカーＩＤ、機器ＩＤ、ＢｋｓｖがＳＴＢのメモリ部に保持しているリボケーションリストに同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

【００６０】

以上のように実施の形態１によれば、ＳＴＢとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーＩＤと機器ＩＤとKSVをＳＴＢのメモリ部に格納してリボケーションリストを作成し、各ＳＴＢからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で、各ＳＴＢよりアップロードされたリボケーションリストを統合した後、セクションにパケット化し、それをＴＳに多重化し、多重されたＴＳを送信部から送出し、送信部から送出されたＴＳをＳＴＢで受信し、統合リボケーションリストを取得することで、もともと各ＳＴＢで個別に所有するリボケーションリストを、全てのＳＴＢで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを

向上させることが可能となる。

【００６１】

（実施の形態２）

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態２について説明する。実施の形態１と異なるのは統合リボケーションリストのパケット化の方法である。図１５に実施の形態２での統合リボケーションリストを含むパケットのデータ構造を示す。実施の形態２では、図１４に示すように、ＭＰＥＧシステム規格のＰＥＳパケットに統合リボケーションリストを格納する。

【００６２】

図１６に実施の形態２における統合リボケーションリストの受信フローを示す。

【００６３】

ステップ３０１において、

ＳＴＢが統合リボケーションリストの格納されたＰＥＳパケットを含むＴＳを受信する。

【００６４】

ステップ３０２において、

ＳＴＢのＴＳデコーダ部１１０４でＴＳから統合リボケーションリストを含むパケットを抽出するように、コントロール部１１０６は、ＴＳデコーダ部１１０４にのＰＩＤフィルタにＲｅｖｏｃａｔｉｏｎ＿ｐｉｄを設定する。

【００６５】

ステップ３０３において、

ＴＳデコーダ部１１０４で統合リボケーションリストを含むパケットを抽出し、コントロール部１１０６が統合リボケーションリストを取得する。

【００６６】

ステップ３０４において、

コントロール部１１０６は取得した統合リボケーションリストを、メモリ部１０７に格納する。

【００６７】

これにより、すべてのＳＴＢで統合リボケーションリストを共有することが可になる。

【００６８】

以上のように実施の形態２によれば、ＳＴＢとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーＩＤ、機器ＩＤ、ＫＳＶをＳＴＢのメモリ部に格納してリボケーションリストを作成し、各ＳＴＢからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で各ＳＴＢよりアップロードされたリボケーションリストを統合した後、ＰＥＳパケットにパケット化し、それをＴＳに多重化し、多重化されたＴＳを送信部から送出し、送信部から送出されたＴＳをＳＴＢで受信し、統合リボケーションリストを取得することで、もともと各ＳＴＢで個別に所有するリボケーションリストを、全てのＳＴＢで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

【００６９】

（実施の形態３）

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態３について説明する。実施の形態１と異なるのは統合リボケーションリストのパケット化の方法である。図１７に実施の形態３での統合リボケーションリストを含むパケットのデータ構造を示す。実施の形態３では、図１７に示すように、ＭＰＥＧシステム規格のＴＳパケットのペイロードにＰＥＳパケットやセクション等のデータ構造をとらずにそのまま統合リボケーションリストを格納する。

【００７０】

図１８に実施の形態３における統合リボケーションリストの受信フローを示す。

【００７１】

ステップ４０１において、

ＳＴＢが統合リボケーションリストの格納されたパケットを含むＴＳを受信する。

【００７２】

ステップ４０２において、

ＳＴＢのＴＳデコーダ部１１０４でＴＳから統合リボケーションを含むパケットを抽出するように、コントロール部１１０６は、ＴＳデコーダ部１１０４のＰＩＤフィルタにＲｅｖｏｃａｔｉｏｎ＿ｐｉｄを設定する。

【００７３】

ステップ４０３において、

ＴＳデコーダ部１１０４で統合リボケーションリストを含むパケットを抽出し、コントロール部１１０６が統合リボケーションリストを取得する。

【００７４】

ステップ４０４において、

コントロール部１１０６は取得した統合リボケーションリストを、メモリ部１１０７に格納する。

【００７５】

これにより、すべてのＳＴＢで統合リボケーションリストを共有することが可になる。

【００７６】

以上のように実施の形態３によれば、ＳＴＢとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーＩＤ、機器ＩＤ、ＫＳＶをＳＴＢのメモリ部に格納してリボケーションリストを作成し、各ＳＴＢからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で各ＳＴＢよりアップロードされたリボケーションリストを統合した後、ＴＳパケットのペイロードに格納することでパケット化し、それをＴＳに多重化し、多重化されたＴＳを送信部から送出し、送信部から送出されたＴＳをＳＴＢで受信し、統合リボケーションリストを取得することで、もともと各ＳＴＢで個別に所有するリボケーションリストを、全てのＳＴＢで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

【００７７】

（実施の形態４）

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態４について説明する。実施の形態１と異なるのは、デジタル放送ではなくインターネット経由で統合リボケーションリストを各ＳＴＢに伝送することである。図１９に実施の形態４におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す。実施の形態１と異なる部分についてのみ説明する。

【００７８】

２０１～２０３はインターネットへのインタフェースを有するＳＴＢである。ＳＴＢ２０１～２０３の内部構成を図２０す。図３に示す実施の形態１のＳＴＢと異なる部分についてのみ説明する。２００１はＬＡＮ　Ｉ／Ｆで後述するネットワークに接続され、ＩＰパケットをやり取りするインタフェースである。

【００７９】

２０４～２０７はインターネットによるネットワークである。２０８は送出センターで、ＩＰパケットに統合リボケーションリストするものである。２０９は送信部で統合リボケーション情報が格納されたＩＰパケットを送出するものである。

【００８０】

以上のように構成された実施の形態４についてその動作を説明する。実施の形態１と異なるものについて説明する。

【００８１】

実施の形態４では、ＳＴＢ２０１～２０３がリボケーションリストを作成するまでは実施の形態１と同一である。図２１ボケーションリストのアップロード～送出までのフローを示す。

【００８２】

ステップ５０１において、

ＳＴＢのコントロール部１１０６が、メモリ部１１０７に格納されたリボケーションリストからメーカーＩＤ、機器ＩＤ、Ｂｋｓｖを読み出し、ＬＡＮ　Ｉ／Ｆ２００１に転送する。

【００８３】

ステップ５０２において

ＳＴＢのＬＡＮ　Ｉ／Ｆ２００１からネットワーク２０４、２０７経由でＢｋｓｖをリボケーションリスト統合部１１４にアップロードする。

【００８４】

ステップ５０３において、

リボケーションリスト統合部１１４において、所定期間に各ＳＴＢからアップロードされたＢｋｓｖの一覧を作成し、これを統合リボケーションリストとする。

【００８５】

ステップ５０４において、

リボケーションリスト統合部１１４から送出センター２０８に統合リボケーションリストを伝送する。

【００８６】

ステップ５０５において、

送出センター２０８で統合リボケーションリストをＩＰパケットに格納する。

【００８７】

ステップ５０６において、

送信部２０９より、統合リボケーションリストが格納されたＩＰパケットを各ＳＴＢに送信する。

【００８８】

ここで、ステップ５０５での統合リボケーションリストのパケット化について説明する。図２２にＩＰパケットのデータ構造の一例を模式的に示す。このパケットのデータの部分に実施の形態１と同様な統合リボケーション情報を格納する。

【００８９】

次に、各ＳＴＢにおける統合リボケーションリストの受信の方法について説明する。図２３にＳＴＢでの統合リボケーションリストの受信フローを示す。

【００９０】

ステップ６０１において、

ＳＴＢがＬＡＮ　Ｉ／Ｆ２００１で統合リボケーションリストを含むＩＰパケットを受信する。

【００９１】

ステップ６０２において、

ＳＴＢのコントロール部１１０６がＬＡＮ　Ｉ／Ｆ２００１から統合リボケーションリストを抽出し、取得する。

【００９２】

ステップ６０３において、

コントロール部１１０６は、取得した統合リボケーションリストをメモリ部１１０７に格納する。

【００９３】

これにより、すべてのＳＴＢで統合リボケーションリストを共有することが可能になる。

【００９４】

そして、新たなディスプレイがＳＴＢに接続された場合に、ディスプレイから読み出した、メーカーＩＤ、機器ＩＤ、ＢｋｓｖがＳＴＢのメモリ部に保持しているリボケーションリストに同一のものがあれば、初期認証は失敗として、以降そのディスプレイを使用できなくする。

【００９５】

以上のように実施の形態４によれば、ＳＴＢとディスプレイの初期認証処理において失敗した場合不正機器とし、その機器のメーカーＩＤ、機器ＩＤ、ＫＳＶをＳＴＢのメモリ部に格納してリボケーションリストを作成し、各ＳＴＢからネットワークを通じてリボケーションリストをリボケーションリスト統合部にアップロードし、リボケーションリスト統合部で各ＳＴＢよりアップロードされたリボケーションリストを統合した後、ＩＰパケットにパケット化し、送信部から送出し、送信部から送出されたＩＰパケットをＳＴＢで受信し、統合リボケーションリストを取得することで、もともと各ＳＴＢで個別に所有するリボケーションリストを、全てのＳＴＢで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

【００９６】

（実施の形態５）

次に本発明のリボケーション情報の送信方法、受信方法の実施の形態５について説明する。図２４に実施の形態５におけるリボケーション情報の送信方法、受信方法を実現するシステムの構成を示す。実施の形態１と異なるのは、リボケーションリストをＳＴＢからアップロードするのではなく、リボケーションリスト統合部３０１で統合リボケーションリストを発行するということである。リボケーションリストは、初期認証の処理が失敗の場合、ユーザがリボケーションリストを管理している機関に連絡をして、リボケーション管理機関はリボケーションリストが格納された機器を回収して、統合リボケーションリストを作成する。統合リボケーションリストは実施の形態１～３のようにＴＳに多重化してもよいし、実施の形態４のようにＩＰパケットに格納してもよい。総合リボケーションリストを作成したあとの処理は実施の形態１～４と同一である。

【００９７】

以上のように本実施の形態５によれば、ＳＴＢからリボケーションリストをアップロードすることなく、リボケーションリスト統合部で統合リボケーションリストを作成し、統合リボケーションリストをＴＳやＩＰパケットに格納し、送信部から送出し、送信部から送出されたＴＳをＳＴＢで受信し、統合リボケーションリストを取得することで、もともと各ＳＴＢで個別に所有するリボケーションリストを、全てのＳＴＢで共有することが可能となり、これにより著作権保護上、不正なディスプレイを排除し、セキュリティを向上させることが可能となる。

【００９８】

なお、以上の実施の形態の説明ではＳＴＢをコンテンツ送出機器として説明したが、ＤＶＤやＰＣなど他の機器であっても構わない。またデジタルインタフェースとして、ＨＤＭＩを例にとって説明したがＤＶＩやＩＥＥＥ１３９４であっても構わない。また、ディスプレイはＡＶスイッチャーなどのリピーター機器であっても構わない。また、統合リボケーションリストはＴＳパケットやＩＰパケット以外のものに格納して伝送しても構わない。またリボケーションリストをアップロードするための手段は、電話やインターネット以外のネットワークであっ

ても構わない。

【００９９】

【発明の効果】

以上のようにこの発明によれば、著作権保護上、不正なディスプレイのリボケーションリストをＳＴＢ等の全ての映像出力機器で共有することで、不正なディスプレイを排除することが可能となり、映像出力機器とディスプレイとを接続するデジタルインタフェースのセキュリティを向上させるという効果を有する。

【図面の簡単な説明】

【図１】

実施の形態１～３におけるリボケーションリストの送信方法、受信方法を実現するシステムを示す図

【図２】

ディスプレイの内部構成を示す図

【図３】

実施の形態１～３におけるＳＴＢの内部構成を示す図

【図４】

デバイスキーの行列を示す図

【図５】

初期認証の処理を示す図

【図６】

ＳＴＢが持つリボケーションリストを示す図

【図７】

ＳＴＢが持つリボケーションリストの作成のフローを示す図

【図８】

更新されたリボケーションリストを示す図

【図９】

実施の形態１～３におけるリボケーションリストのアップロード～統合リボケーションリスト送出までのフローを示す図

【図１０】

トランスポートパケットのデータ構造を模式的に示す図

【図１１】

トランスポートパケットのデータ構造を示す図

【図１２】

統合リボケーションリストをセクション構造に格納した場合のデータ構造を示す図

【図１３】

実施の形態１の統合リボケーションリストの受信フローを示す図

【図１４】

各ＳＴＢで共有される統合リボケーションリストを示す図

【図１５】

統合リボケーションリストをＰＥＳパケット構造に格納した場合のデータ構造を示す図

【図１６】

実施の形態２における統合リボケーションリストの受信フローを示す図

【図１７】

統合リボケーションリストをトラスポートパケットのペイロードに格納した場合のデータ構造を示す図

【図１８】

実施の形態３における統合リボケーションリストの受信フローを示す図

【図１９】

実施の形態４におけるリボケーションリストの送信方法、受信方法を実現するシステム装置を示す図

【図２０】

実施の形態４におけるＳＴＢの内部構成を示す図

【図２１】

実施の形態４におけるリボケーションリストのアップロード～統合リボケーションリスト送出までのフローを示す図

【図２２】

ＩＰパケットのデータ構造を示す図

【図２３】

実施の形態４における統合リボケーションリストの受信フローを示す図

【図２４】

実施の形態５おけるリボケーションリストの送信方法、受信方法を実現するシステム装置を示す図

【図２５】

従来例を示す図

【符号の説明】

１０１　第1のディスプレイ

１０２　第1のＳＴＢ

１０３　第１のデジタルインタフェース

１０４　第２のディスプレイ

１０５　第２のＳＴＢ

１０６　第２のデジタルインタフェース

１０７　第Ｎのディスプレイ

１０８　第ＮのＳＴＢ

１０９　第Ｎのデジタルインタフェース

１１０　第1の上り回線

１１１　第２の上り回線

１１２　第Ｎの上り回線

１１３　ネットワーク

１１４　リボケーションリスト統合部

１１５　送出センター

１１６　送信部

１００１　表示部

１００２　機器インタフェース

１００３　コントロール部

１００４　メモリ部

１１０１　アンテナ

１１０２　チューナ部

１１０３　フロントエンド部

１１０４　ＴＳデコーダ部

１１０５　ＡＶデコーダ部

１１０６　コントロール部

１１０７　メモリ部

１１０８　ディスプレイインタフェース

２０１　第1のＳＴＢ

２０２　第２のＳＴＢ

２０３　第ＮのＳＴＢ

２０４～２０７　ネットワーク

２０８　送出センター

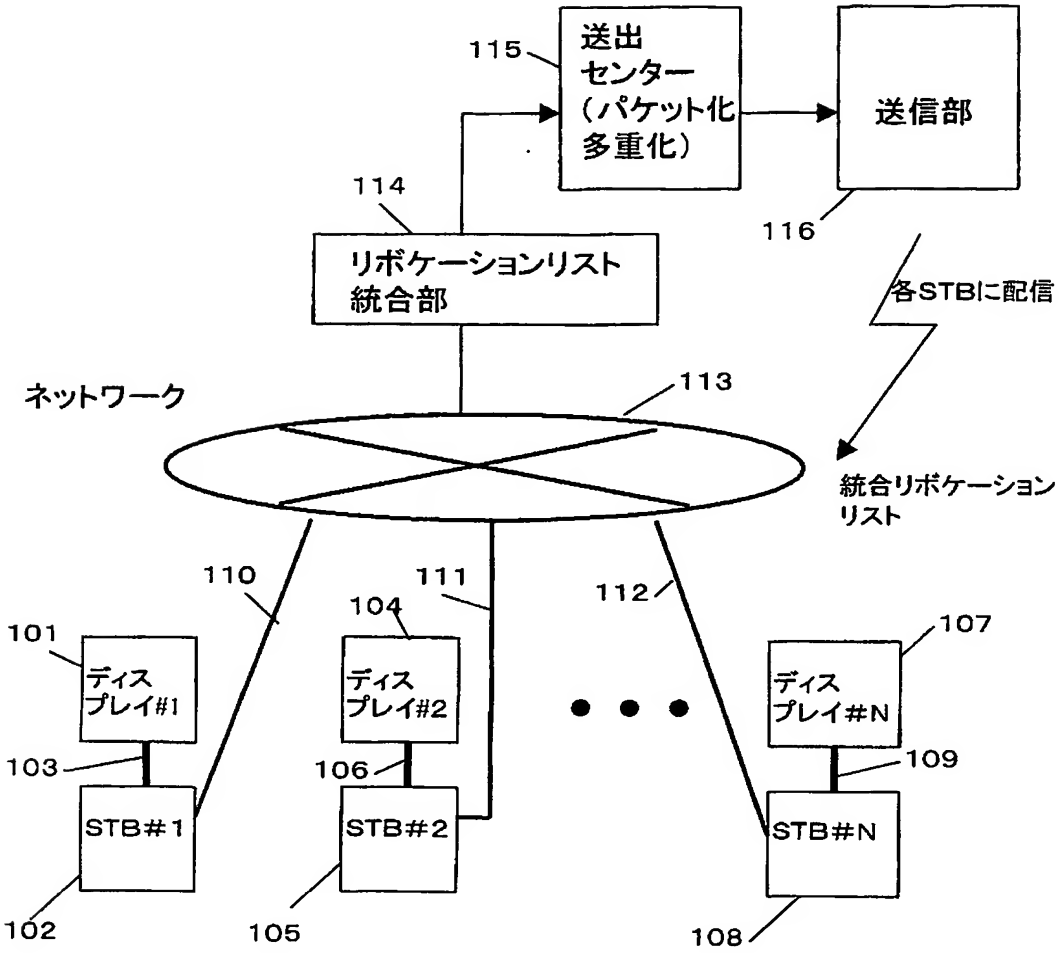
２０９　送信部

２００１　ＬＡＮ　Ｉ／Ｆ

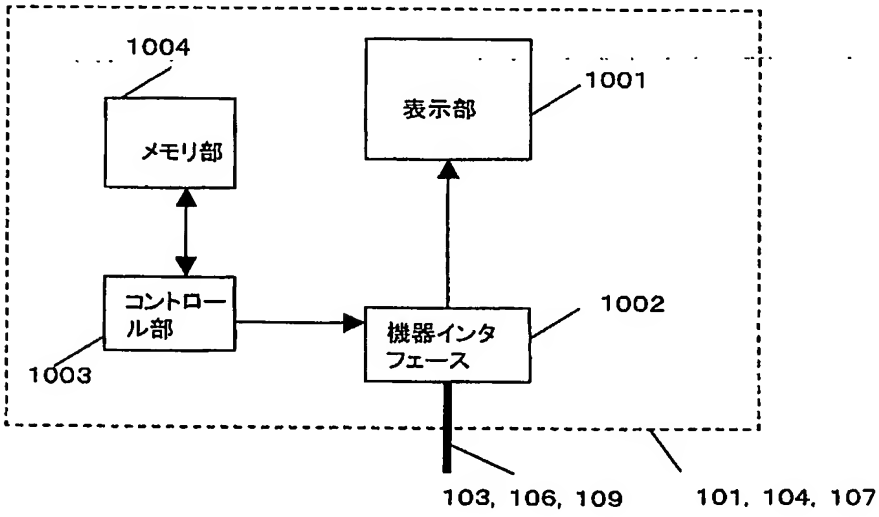
３０１　リボケーションリスト統合部

【書類名】　図面

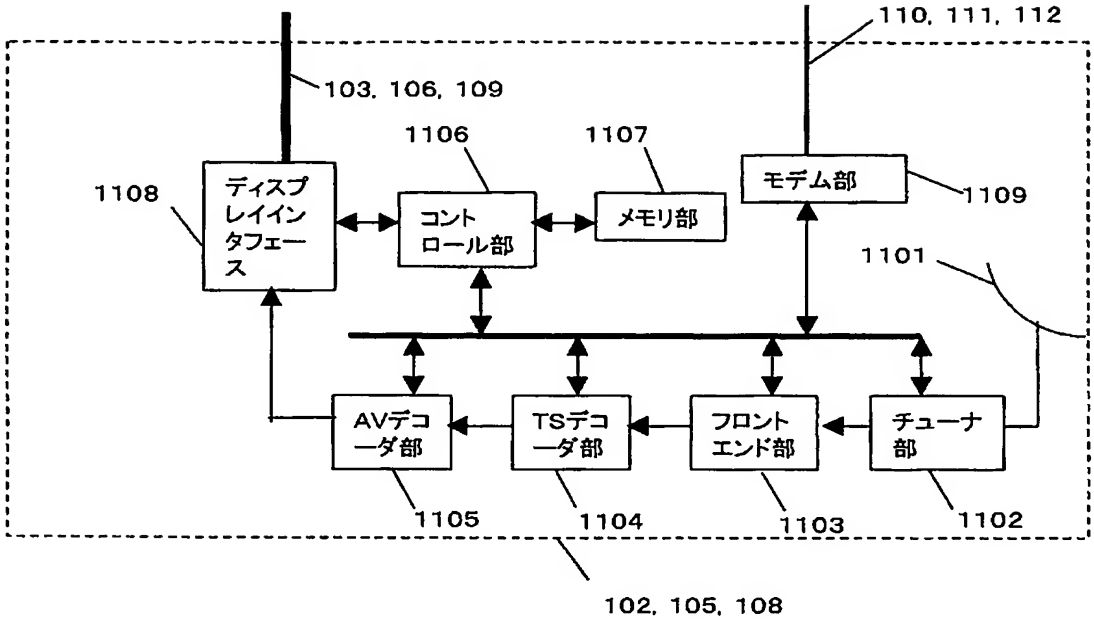
【図１】


115
送出
センター
（パケット化
多重化）
送信部
114
116
リボケーションリスト
統合部
各STBに配信
ネットワーク
113
統合リボケーション
リスト
110
111
112
104
101
107
ディス
プレイ#1
ディス
プレイ#2
ディス
プレイ#N
103
106
109
STB#１
STB#２
STB#N
102
105
108

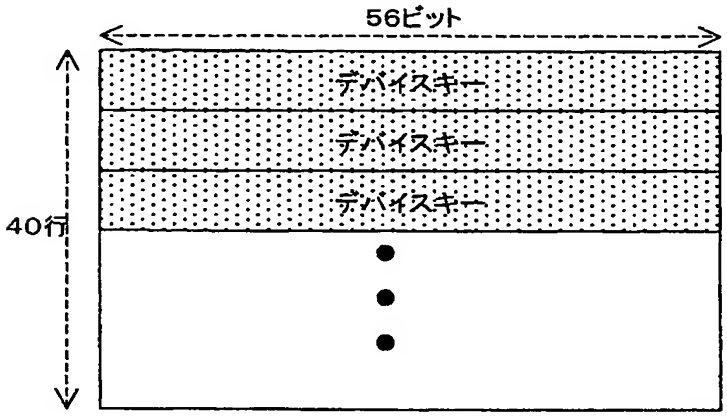
【図２】


1004
表示部
1001
メモリ部
コントロー
ル部
1002
機器インタ
フェース
1003
103, 106, 109
101, 104, 107

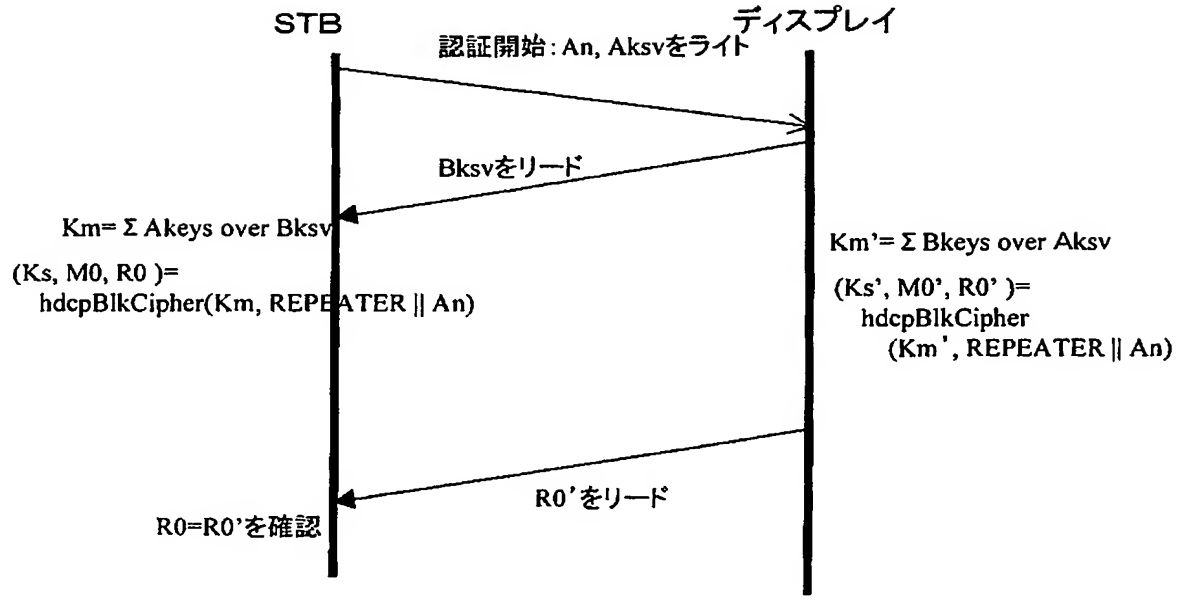
【図３】


110, 111, 112
103, 106, 109
1106
1107
1108
ディスプレイインタフェース
コントロール部
メモリ部
モデム部
1109
1101
AVデコーダ部
TSデコーダ部
フロントエンド部
チューナ部
1105
1104
1103
1102
102, 105, 108

【図４】


56ビット
デバイスキー
デバイスキー
デバイスキー
40行

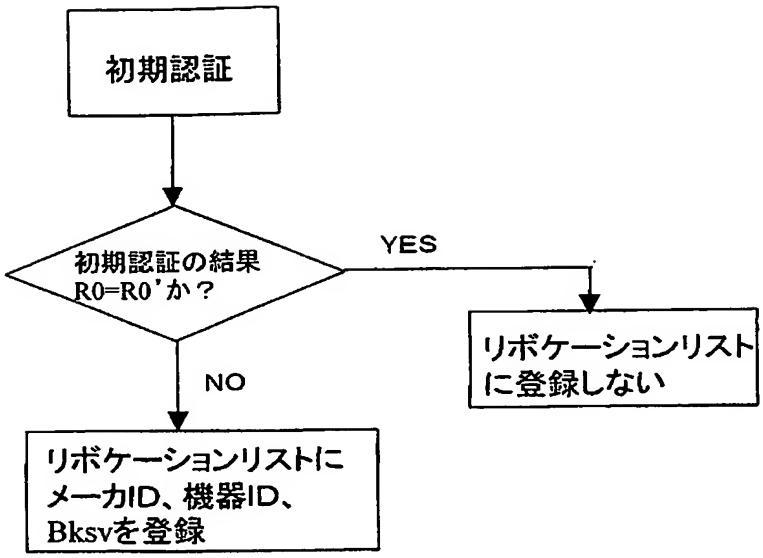
【図５】



【図６】

メーカーID	機器ID	Bksv
maker_1	kiki_1	Bksv_1
maker_2	kiki_2	Bksv_2
無登録	無登録	無登録
無登録	無登録	無登録

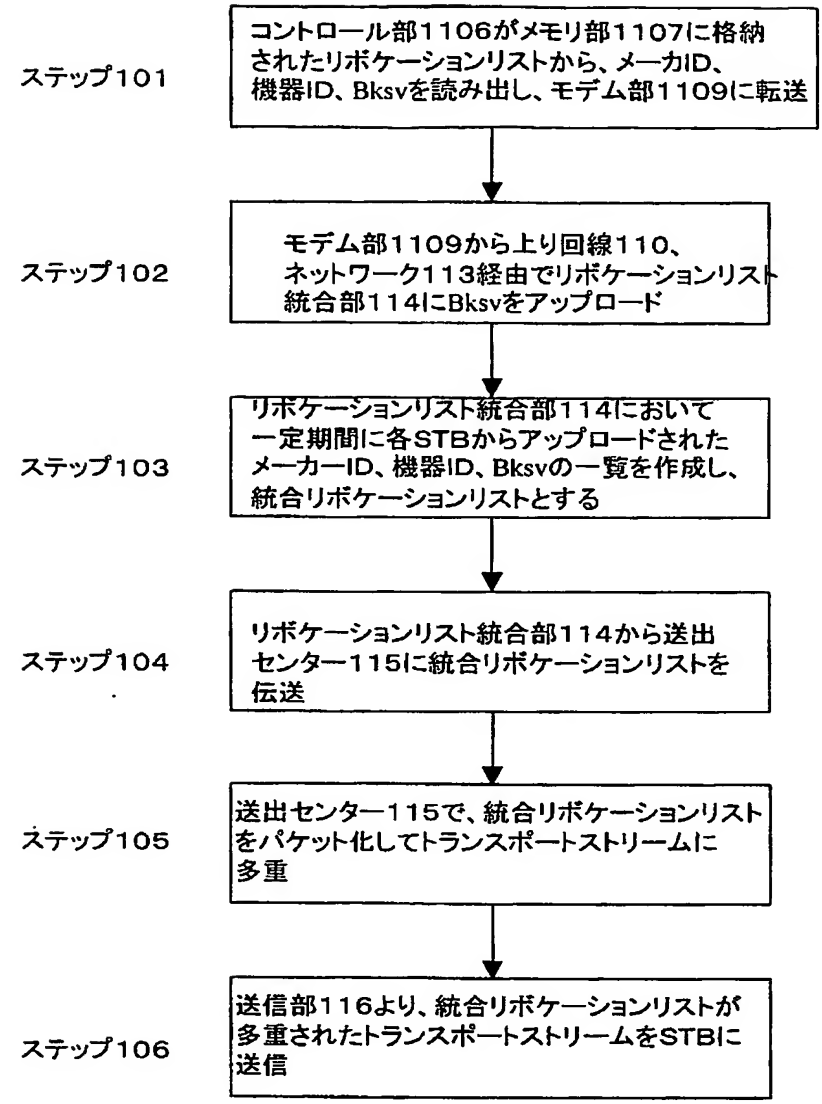
【図７】



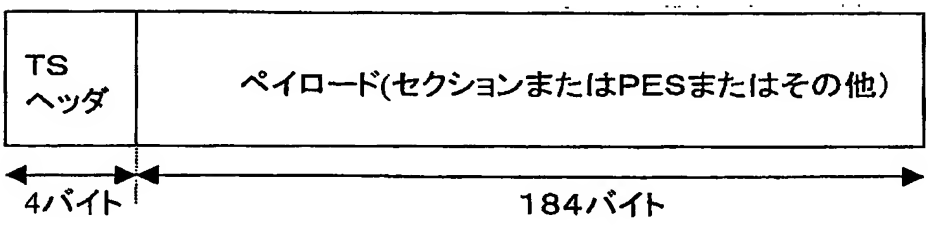
【図８】

メーカーID	機器ID	Bksv
maker_1	kiki_1	Bksv_1
maker_2	kiki_2	Bksv_2
maker_3	kiki_3	Bksv_3
無登録	無登録	無登録

【図９】


ステップ101
コントロール部1106がメモリ部1107に格納されたリボケーションリストから、メーカID、機器ID、Bksvを読み出し、モデム部1109に転送
ステップ102
モデム部1109から上り回線110、ネットワーク113経由でリボケーションリスト統合部114にBksvをアップロード
ステップ103
リボケーションリスト統合部114において一定期間に各STBからアップロードされたメーカーID、機器ID、Bksvの一覧を作成し、統合リボケーションリストとする
ステップ104
リボケーションリスト統合部114から送出センター115に統合リボケーションリストを伝送
ステップ105
送出センター115で、統合リボケーションリストをパケット化してトランスポートストリームに多重
ステップ106
送信部116より、統合リボケーションリストが多重されたトランスポートストリームをSTBに送信

【図１０】


TS
ヘッダ
ペイロード(セクションまたはPESまたはその他)
4バイト
184バイト

【図１１】

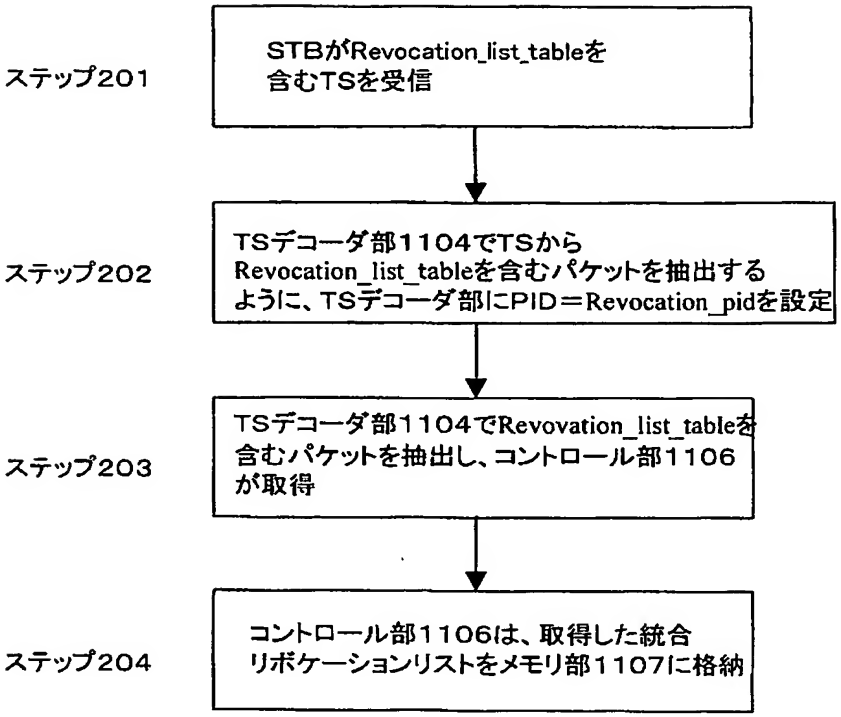
フィールド	ビット数
sync_byte	8
transport_stream_indicatior	1
payload_unit_start_indicator	1
tranport_priority	1
PID	13
transport_scrambling_cintrol	2
adaptation_field_control	2
continuity_counter	4
for (i=0; i <n; i++){	
data_byte	8
}	

【図１２】

Revocation_List_Table

フィールド	ビット数
table_id	8
section_syntax_indicatior	1
reserved	2
section_length	12
program_number	16
reserved	2
version_number	5
current_next_indicator	1
section_number	8
last_section_number	8
for(i=0; i<n; i++){	
maker_id	16
kiki_id	32
device_KSV	40
}	
CRC_32	32

【図１３】



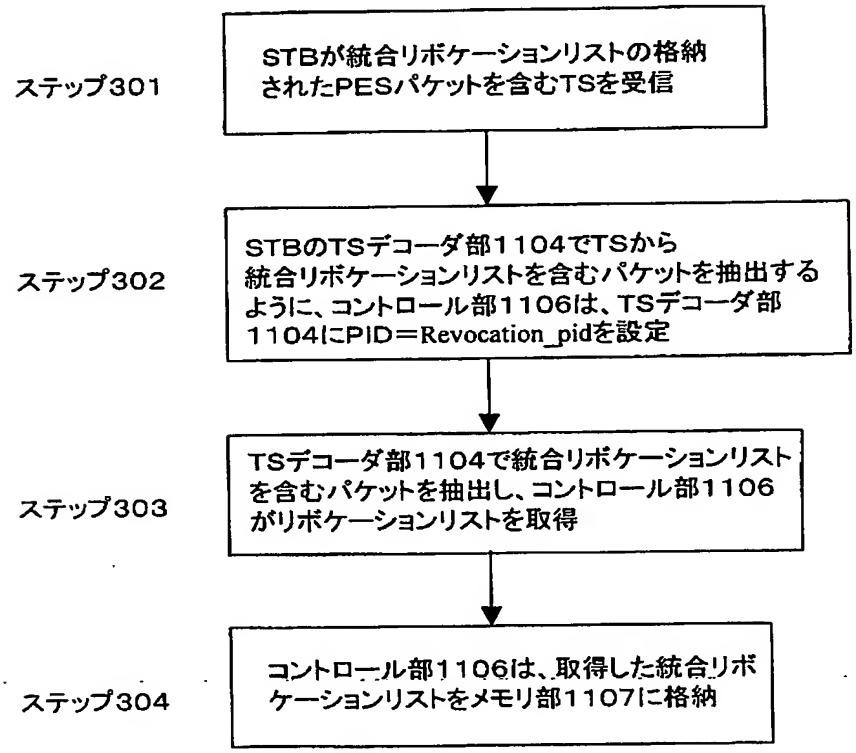
【図１４】

メーカーID	機器ID	Bksv
maker_1	kiki_1	Bksv_1
maker_2	kiki_2	Bksv_2
maker_3	kiki_3	Bksv_3
maker_4	kiki_4	Bksv_4
maker_5	kiki_5	Bksv_5
無登録	無登録	無登録
無登録	無登録	無登録

【図１５】

フィールド	ビット数
packet_start_code_prefix	24
strem_id	8
PES_packet_lengh	16
for (i=0; i<PES_packet_length/5; i++){	
maker_id	16
kiki_id	32
device_KSV	40
}	

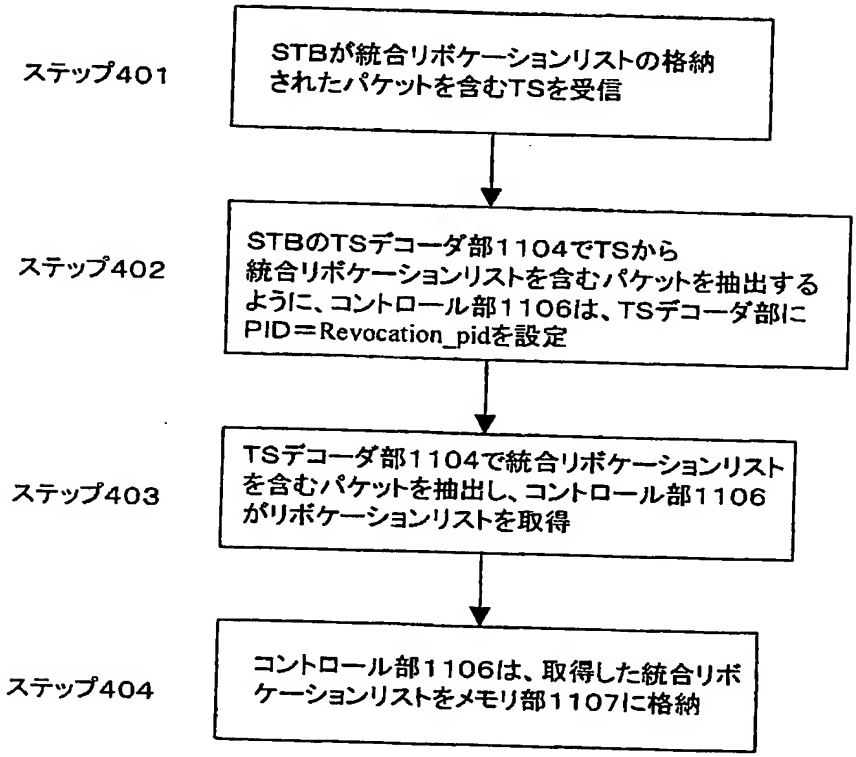
【図１６】



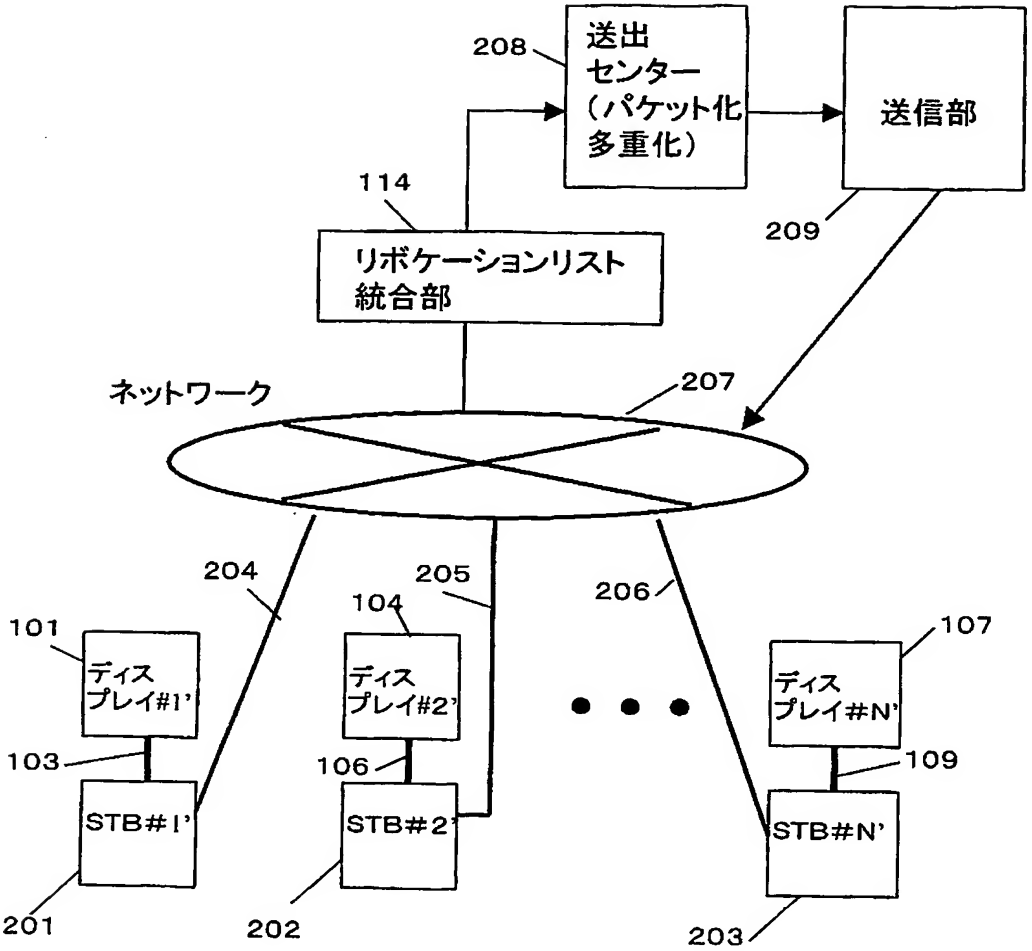
【図１７】

フィールド	ビット数
KSV_number	16
For (I=0; I<KSV_number; I++){	
maker_id	16
kiki_id	32
device_KSV	40
}	

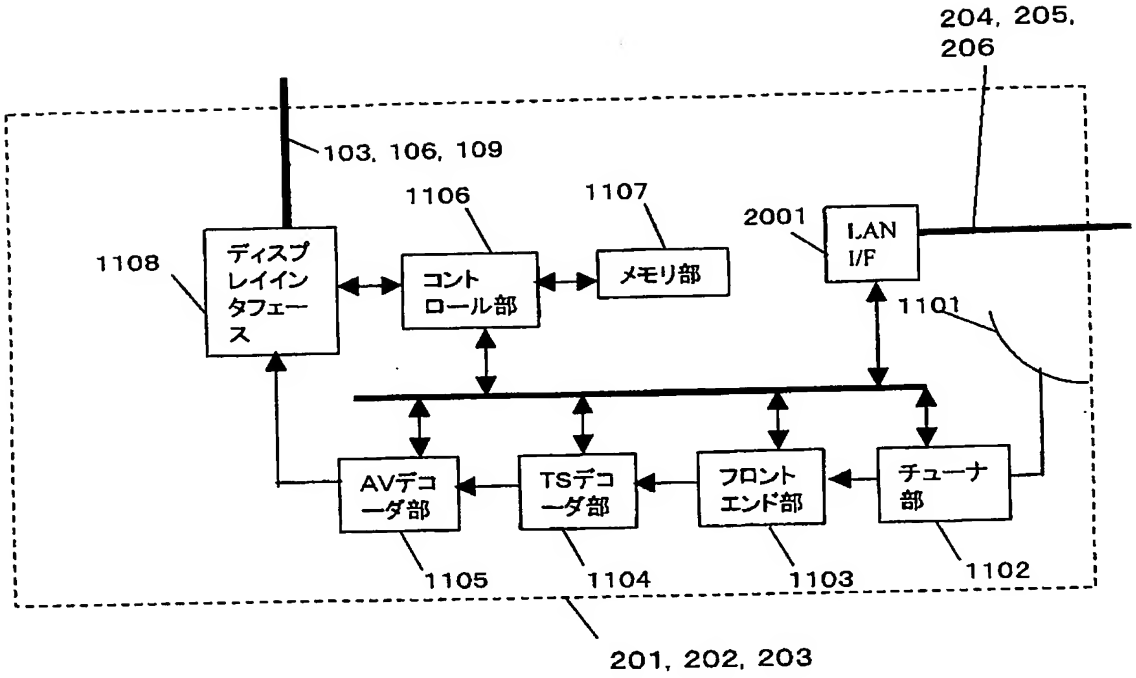
【図１８】



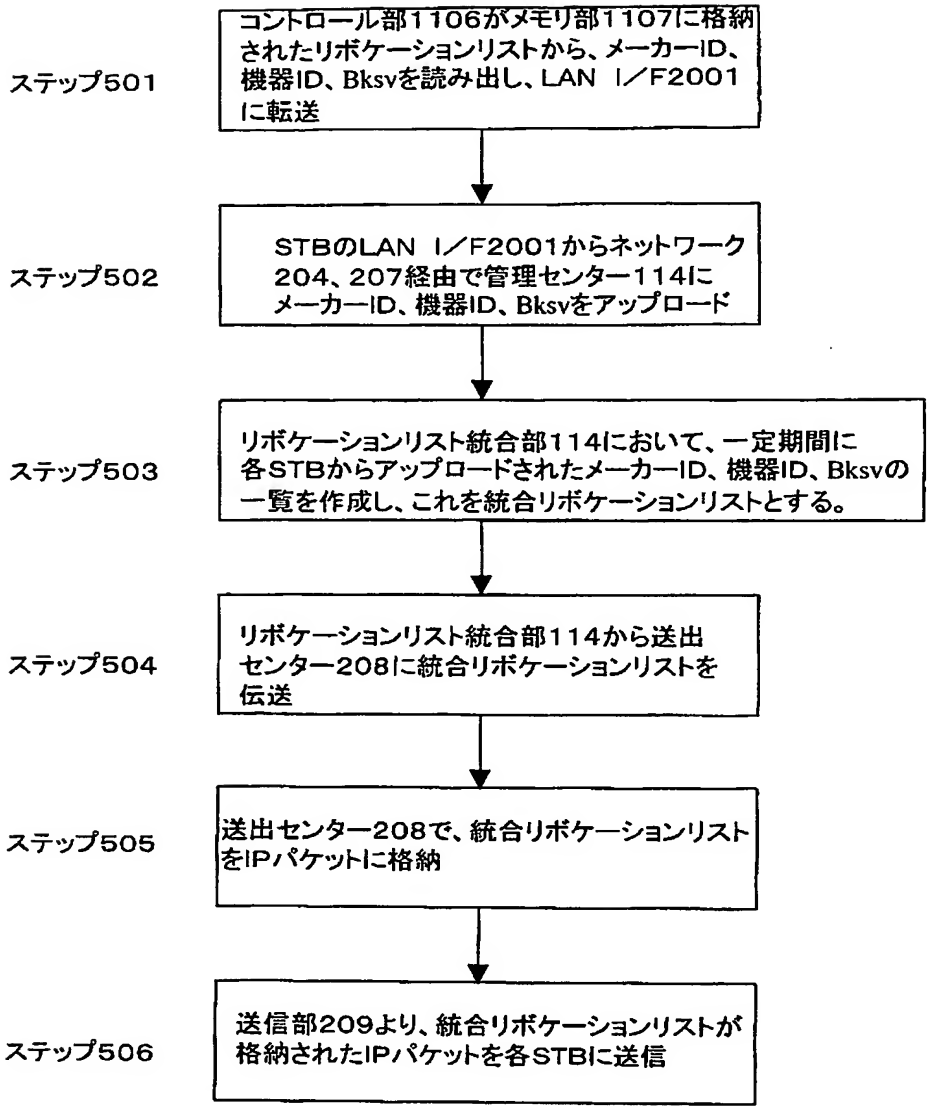
【図１９】


208
送出
センター
（パケット化
多重化）
送信部
114
209
リボケーションリスト
統合部
ネットワーク
207
204
205
206
104
101
107
ディス
プレイ#1’
ディス
プレイ#2’
ディス
プレイ#N’
103
106
109
STB#1’
STB#2’
STB#N’
201
202
203

【図２０】


204, 205, 206
103, 106, 109
1106
1107
2001
LAN I/F
1108
ディスプレイインタフェース
コントロール部
メモリ部
1101
AVデコーダ部
TSデコーダ部
フロントエンド部
チューナ部
1105
1104
1103
1102
201, 202, 203

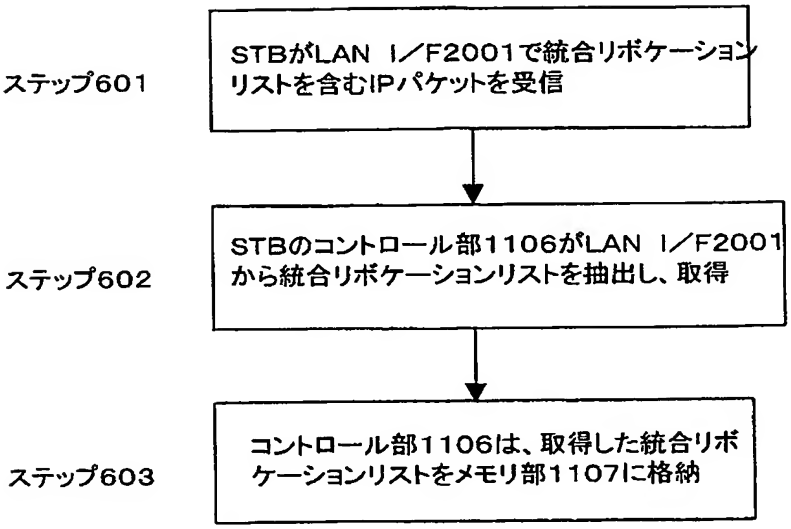
【図２１】



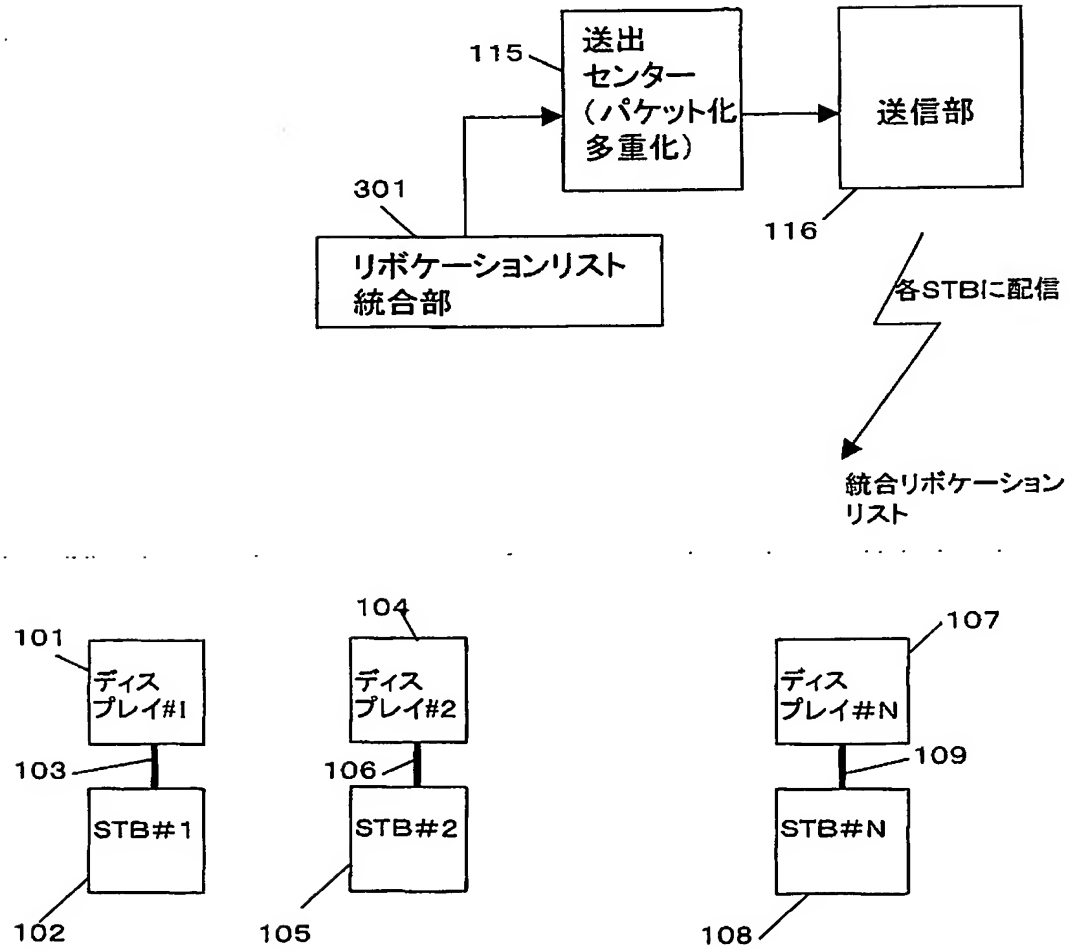
【図２２】

送信元IPアドレス	送信先IPアドレス	プロトコルタイプ	送信元ポート番号	送信先ポート番号	データ	FCS

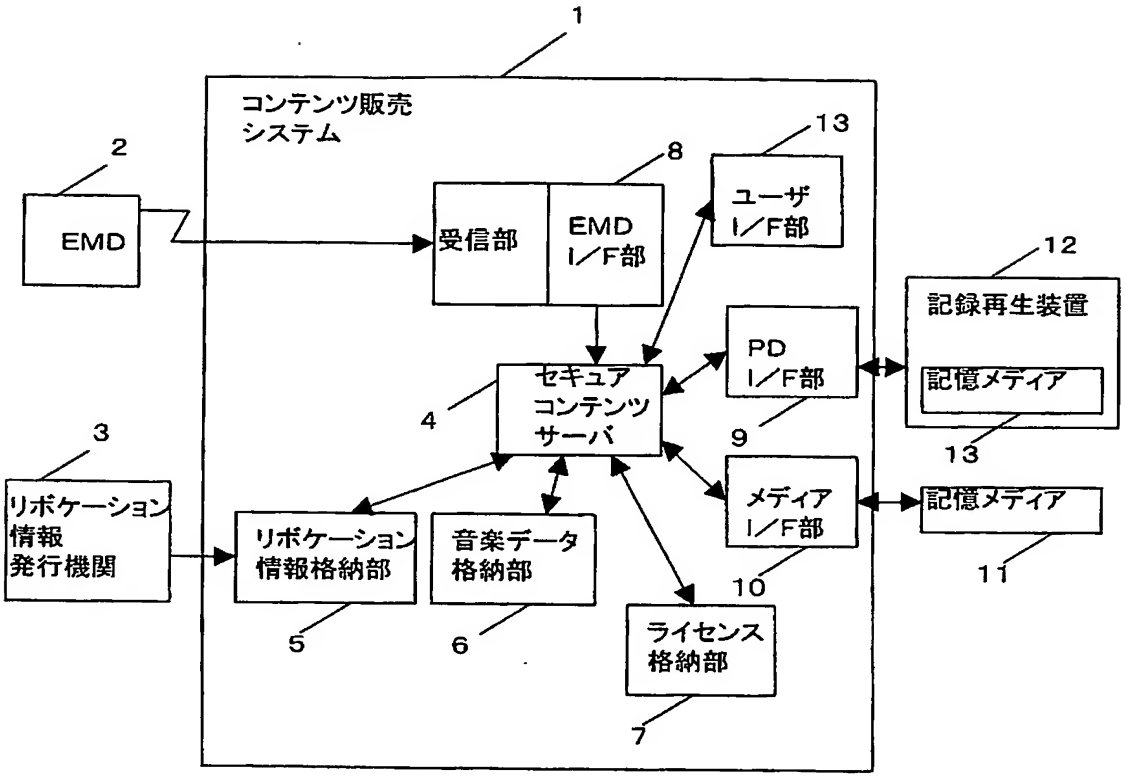
【図２３】


ステップ601
STBがLAN I／F2001で統合リボケーションリストを含むIPパケットを受信
ステップ602
STBのコントロール部1106がLAN I／F2001から統合リボケーションリストを抽出し、取得
ステップ603
コントロール部1106は、取得した統合リボケーションリストをメモリ部1107に格納

【図２４】


115
送出センター（パケット化多重化）
送信部
301
116
リボケーションリスト統合部
各STBに配信
統合リボケーションリスト
101
ディスプレイ#1
103
STB#1
102
104
ディスプレイ#2
106
STB#2
105
107
ディスプレイ#N
109
STB#N
108

【図２５】


1
コンテンツ販売
システム
2
EMD
8
受信部
EMD
I／F部
13
ユーザ
I／F部
12
記録再生装置
記憶メディア
PD
I／F部
4
セキュア
コンテンツ
サーバ
9
3
リポケーション
情報
発行機関
メディア
I／F部
記憶メディア
13
11
10
リポケーション
情報格納部
音楽データ
格納部
ライセンス
格納部
5
6
7

【書類名】　要約書

【要約】

【課題】　著作権上排除すべき不正機器のリボケーション情報はそれに接続された機器にしか記憶されない。接続されうる全ての機器に対してリボケーション情報を配布してリボケーション情報を共有して不正機器を排除する必要がある。

【解決手段】　コンテンツ送出機器／受信機器と、それらを接続する接続手段から構成されるシステムにおいて、コンテンツ送出機器とコンテンツ受信機器が相互認証を行なうステップと、相互認証が失敗の場合、失敗した鍵情報を含むリボケーション情報をネットワークにアップロードするステップと、複数のコンテンツ送出機器またはコンテンツ受信機器からアップロードされた個々のリボケーション情報を統合して統合リボケーション情報を作成するステップと、統合リボケーション情報をパケット化し、ストリームに多重するステップと、統合リボケーションが多重されたストリームを送出するステップを備えることを特徴とする。

【選択図】　図１

特願２００３－０８５０４３

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社